STATEMENT OF SENATOR DANIEL K. AKAKA
In Support of S. 1993, the Government Information Security Act
Senate Governmental Affairs Committee
March 23, 2000

I am pleased to cosponsor S. 1993, the Government Information Security Act, which will strengthen the federal government's critical computer infrastructure. This bipartisan measure, introduced by our Chairman and Ranking Member, provides a framework for how the government could make its systems more secure while simultaneously providing continuous, uninterrupted services to the public.

I am delighted that the bill's sponsors accepted my amendment, which will ensure full government compliance and accountability and promote public confidence by linking the requirements of S. 1993 to the Government Performance Results Act.

The indefensible state of critical infrastructure security within the federal government places our nation at extraordinary risk. As the ranking member of the Governmental Affair's Subcommittee on International Security, Proliferation, and Federal Services, I wish to call attention to the sub-par performance of many key executive departments. Despite the numerous hearings this Committee has held on computer infrastructure protection, the level of protection accorded some of the government's most sensitive networks is abysmal, even after several years of aggressive efforts to improve the situation.

Since the early 1990s, there has been an explosive growth in computer connectivity throughout all levels of government and industry. This growth has been furthered by the virtually unlimited access provided by the Internet. The many benefits derived from this phenomenal growth include, but are not limited to, increased efficiencies, cost savings and unprecedented speed and range of access to information. Nevertheless, there is a dark side to this unfettered growth that without decisive action may have profound consequences - a cataclysmic attack on our nation's infrastructure.

President Clinton's recently announced National Plan for Information Systems Protection and S. 1993 appropriately identify important steps necessary to mitigate long-standing acute vulnerabilities. Unfortunately full implementation of new plans and passage of legislation takes time. Because the threat is so severe, and the detrimental consequences of accepting the status quo are so profound, that Congress must take immediate action. The bipartisan General Accounting Office (GAO) has determined that 22 of the largest federal agencies are not adequately protecting critical federal operations and assets from computer-based attacks, despite current regulations and policies, which if adhered to, would provide significantly greater protection than now exists. GAO audits have demonstrated that federal agencies have not done enough with existing authorities and resources to mitigate this growing threat.

Over the past five years, the General Accounting Office and the Federal Inspector Generals (IG) community have conducted innumerable audits and "controlled penetration tests" of government networks. Their findings have been nothing short of startling. These include:

- After repeated audits of the Department of Defense infrastructure, in 1999, the GAO reported serious weaknesses in information security which continues to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose and destroy sensitive DOD data. Numerous Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll have already been adversely affected by systems attack and fraud.

- In 1998, the GAO concluded that the State Department's information systems are vulnerable to access, change, disclosure, disruption and even denial of service by unauthorized individuals. The GAO concluded that top managers at State have not demonstrated that they are committed to strengthening security over the systems they rely on for nearly every aspect of State's operations.

- Perhaps most disturbingly, during a May 1999 evaluation of the National Aeronautics and Space Administration (NASA), the GAO was able to penetrate several mission critical systems, including one responsible for calculating detailed positioning data for earth orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft. The GAO report found that NASA's mission-critical systems were vulnerable to unauthorized access and sabotage and their data to theft, modification, and destruction. This was attributed to significant management shortcomings in every aspect of NASA's information technology (IT) security program.

During recent Governmental Affairs Committee hearings, an infamous computer hacker attributed his near universal success at penetrating every network he targeted to his non-technical ability to obtain sensitive systems access information, such as passwords, through a tactic he termed "social engineering." Social engineering includes misrepresentation, trickery, intimidation or shear bravado to convince others to provide privileged access to information and/or spaces. The GAO was no less successful in its efforts to apply far less aggressive tactics in exploiting poor personnel security practices to gain easy, nearly undetectable, unauthorized access to some of the government's most sensitive systems.

The Committee heard testimony regarding ever evolving technical vulnerabilities inherit in the flaws of software, hardware and networks used within the public and private sectors. The scope of the problem is daunting. We know that every day there are thousands of unsuccessful attempts made to hack into government and private networks, but the number of successful unlawful penetrations remains largely unknown. We also know that there are scores of countries, and untold numbers of terrorist and/or organized criminal groups, who have, or are developing offensive cyber capabilities. In short, cyber crime is flourishing, cyber terrorism and cyber warfare are largely untested, but will undoubtedly soon follow - perhaps with devastating consequences.

It is particularly disturbing to note that virtually every federal executive department that GAO has assessed has been found to be deficient. Many have continually failed to institute fundamental government mandates and/or universally recognized security safeguards even after past deficiencies were surfaced. As a consequence, federal systems remain highly and unnecessarily vulnerable to unauthorized access and sabotage and their sensitive data to theft, modification and destruction.

New laws and programs are necessary to keep pace with this evolving threat, but we do not need new laws or programs to insist that government officials take common sense steps, already within their purview, to fulfill their obligation to protect the public trust. The Inspector Generals of each of the 22 Federal agencies cited by the GAO with computer securities deficiencies should now be taking sufficient steps to ensure infrastructure protection programs are at least brought up to current standards. We well know the severe damage an unsophisticated but determined hacker can wreak on the most protected networks, much less networks replete with the pronounced systemic vulnerabilities endemic to federal systems.

I will continue to support the President's computer security plan and quick enactment of S. 1993, the Government Information Security Act.